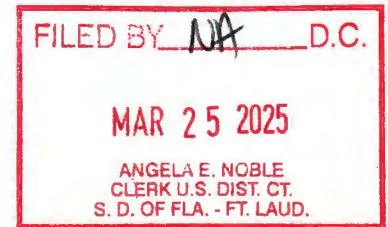


UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF FLORIDA



UNITED STATES OF AMERICA,  
Plaintiff,

v.

SANJAY SINGH,  
Defendant.

Case No.: 0:23-cr-60117-DSL

**DEFENDANT'S MOTION TO UNSEAL GRAND JURY TRANSCRIPTS**

**COMES NOW**, the Defendant, **Sanjay Singh**, as PRO-SE and respectfully moves this Court to order the unsealing and disclosure of the grand jury transcripts in this case. The **particularized need** for disclosure of the grand jury materials **outweighs the presumption of grand jury secrecy** in the interest of justice. This request is made pursuant to **Federal Rule of Criminal Procedure 6(e)(3)(E)(i)-(ii)** and in support thereof, Defendant states as follows:

---

**I. INTRODUCTION**

Case No.: 0:23-cr-60117-DSL

The differential between the indictment (see..ECF 1)and the search warrant (see EXHIBIT SA)affidavit authored by Austin Steelman raises substantial constitutional concerns regarding the Fourth, Fifth, and Sixth Amendments. Given the discrepancies between the allegations in the indictment and the representations in the search warrant affidavit, there exists a possible ground to dismiss the indictment on constitutional grounds.

Additionally, disclosure of grand jury material is necessary in connection with the judicial proceeding for the sentencing of Sanjay Singh on April 15, 2025, where evidence of constitutional violations before the grand jury may impact sentencing determinations.

For these reasons, the interest of justice requires disclosure of the grand jury transcripts.

---

## II. LEGAL STANDARD

Federal Rule of Criminal Procedure 6(e)(3)(E)(i)-(ii) allows for the disclosure of grand jury materials:

1. **When a party demonstrates a particularized need** for the material that outweighs the need for secrecy (*Douglas Oil Co. of California v. Petrol Stops Northwest*, 441 U.S. 211, 223 (1979)).
2. **When the disclosure is sought in connection with a judicial proceeding** (*United States v. Aisenberg*, 358 F.3d 1327, 1348 (11th Cir. 2004)).

The Eleventh Circuit has held that grand jury secrecy **must yield** when disclosure is necessary to **ensure fundamental fairness** and prevent injustice (*In re Grand Jury Proceedings*, 4 F.3d 1153, 1156 (11th Cir. 1993)).

A **particularized need exists** when a defendant shows:

- A **potential constitutional violation** affecting the grand jury's decision.
- A **differential between the indictment and other sworn statements** suggesting misconduct.
- A **direct impact on sentencing or post-conviction rights**.

Here, all these factors weigh in favor of unsealing the grand jury transcripts.

---

### **III. PARTICULARIZED NEED JUSTIFYING DISCLOSURE**

#### **1. The Differential Between the Indictment and the Search Warrant Affidavit Suggests Possible Fourth, Fifth, and Sixth Amendment Violations**

The indictment **alleges fraudulent misrepresentations and omissions**, but the search warrant **affidavit presents a different factual narrative**, particularly concerning **title fraud, business mismanagement, and omissions without a legal duty to disclose**.

This inconsistency raises concerns that:



- The **grand jury** may have been presented with misleading or incomplete information.
- The **indictment** may have been obtained based on legally insufficient evidence, violating **Due Process under the Fifth Amendment**.
- There may have been **Fourth Amendment violations** related to the use of potentially misleading statements in obtaining evidence.
- **Sixth Amendment concerns** arise if the grand jury proceedings **improperly limited the defense's ability to challenge evidence later used at trial**.

Under *Bank of Nova Scotia v. United States*, 487 U.S. 250 (1988), a **dismissal of an indictment is warranted when a defendant can show that a constitutional violation undermined the grand jury process**. Here, unsealing the transcripts is necessary to determine whether the indictment was **constitutionally defective**.

## **2. Grand Jury Material is Necessary for the Sentencing Hearing on April 15, 2025**

Under *United States v. Pantoja*, 965 F.2d 793 (11th Cir. 1992), disclosure is warranted **when grand jury material is necessary for an upcoming judicial proceeding**. The upcoming sentencing hearing for **Sanjay Singh on April 15, 2025**, is directly impacted by:

- Whether the grand jury was **misled into issuing an indictment based on unconstitutional evidence**.
- Whether **prosecutorial misconduct before the grand jury violated Singh's Due Process rights**, warranting a **reduced sentence or dismissal of certain counts**.

The **sentencing court has discretion to consider the fairness of the grand jury process** (*United States v. Accetturo*, 966 F.2d 631, 635 (11th Cir. 1992)). Without disclosure of the grand jury transcripts, **Singh will be deprived of his ability to challenge constitutional violations affecting his sentencing.**

---

#### **IV. BALANCING THE INTERESTS: JUSTICE OVER SECRECY**

While grand jury secrecy serves an important function, **secrecy must yield when disclosure is required to prevent injustice** (*United States v. Sells Engineering, Inc.*, 463 U.S. 418, 428 (1983)).

Here, disclosure is necessary because:

- The **differential between the indictment and the search warrant affidavit suggests that the grand jury may have been misled.**
- The **Fourth, Fifth, and Sixth Amendment violations require disclosure to ensure Due Process.**
- The **impact of these violations extends beyond indictment to sentencing, necessitating judicial review.**

Thus, the **particularized need for transparency outweighs the general need for secrecy.**

#### **V. CONCLUSION**

For the foregoing reasons, Defendant **Sanjay Singh** respectfully requests that this Court **order the unsealing and disclosure of the grand jury transcripts** in this case. The **constitutional concerns, discrepancies between the indictment and search warrant affidavit**, and the **upcoming sentencing hearing** all justify disclosure in the **interest of justice**.

**WHEREFORE**, Defendant respectfully requests that this Court grant this Motion and **order the immediate unsealing of the grand jury transcripts**.

## **VII. CERTIFICATE OF CONFERENCE**

A good faith effort was made with the government through public defender office. No response received other than status conference set for April 8<sup>th</sup>, 2025.

## **VIII. CERTIFICATE OF SERVICE**

A paper copy has been mailed to Clerk of Court and will be filed by CM/ECF system all parties will receive a copy electronically.

If hand signature required Defendant is available in court room only for signature.

**Dated:** March 24, 2025

**Respectfully submitted,**

S/Sanjay Singh in custody US MARSHAL

EMAIL: [SJAYSINGH@ICLOUD.COM](mailto:SJAYSINGH@ICLOUD.COM)

SHEETAL SINGH  
(352) 421-1879  
THE UPS STORE #7550  
6288 W SAMPLE RD #403  
CORAL SPRINGS FL 33067-3272

1 LBS 1 OF 1  
SHIP WT: 1 LBS  
DATE: 24 MAR 2025

SHIP US DISTRICT COURT CLERK  
TO: STE 108  
299 E BROWARD BLVD

FORT LAUDERDALE FL 33301-1922



FL 333 0-02



UPS GROUND

TRACKING #: 1Z A59 A90 03 0160 3456



BILLING: P/P

REF 01: AH

HN4HAB1JHFRH 10H 15.00P Z2P 400 00.00 03/2025



SEE NOTICE ON RETURN regarding UPS Terms, and notice of limitation of liability. Where allowed by law, shipper authorizes UPS to act as forwarding agent for export control and customs purposes. If required from the US, shipper certifies that the commodities, technology or software were exported from the US in accordance with the Export Administration Regulations. Otherwise, country to law is prohibited.

800 8 1234



US DISTRICT COURT CLERK  
299 E BROWARD BLVD  
STE 108  
FORT LAUDERDALE FL 33301

P:BLUE S:RIGHT I:18E

47-6180

1ZA59A90030160 3456  
SAT08485 XLE 02-1 Rev 25 06:52:30 2025  
US 3331 HIPPS 25.3.2 SATOLR





# **EXHIBIT SA**

FILED BY SM D.C.

**Jun 9, 2023**

ANGELA E. NOBLE  
CLERK U.S. DIST. CT.  
S. D. OF FLA. - FTL

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 23-MJ-6256-PAB

IN RE: SEALED SEARCH WARRANT  
\_\_\_\_\_ /

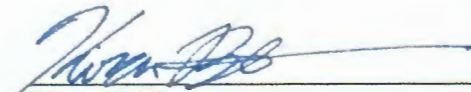
**CRIMINAL COVER SHEET**

1. Did this matter originate from a matter pending in the Northern Region of the United States Attorney's Office prior to August 8, 2014 (Mag. Judge Shaniek Maynard)? \_\_\_ Yes X No
2. Did this matter originate from a matter pending in the Central Region of the United States Attorney's Office prior to October 3, 2019 (Mag. Judge Jared Strauss)? \_\_\_ Yes X No
3. Did this matter involve the participation of or consultation with now Magistrate Judge Eduardo I. Sanchez during his tenure at the U.S. Attorney's Office, which concluded on January 22, 2023? \_\_\_ Yes X No

Respectfully submitted,

MARKENZY LAPOINTE  
UNITED STATES ATTORNEY

By:

  
Kiran N. Bhat

Assistant United States Attorney  
Florida Bar No. 1008370  
99 NE 4th Street, 4th Floor  
Miami, Florida 33132  
Tel: (305) 961-9103  
kiran.bhat@usdoj.gov

FILED BY SM D.C.

**Jun 9, 2023**

ANGELA E. NOBLE  
CLERK U.S. DIST. CT.  
S. D. OF FLA. - FTL

**UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF FLORIDA**

**CASE NO. 23-MJ-6256-PAB**

**IN RE: SEALED SEARCH WARRANT**

---

**MOTION TO SEAL**

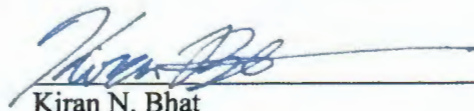
The United States of America requests that the Application and Affidavit for Search Warrant, Attachments to the Application and Search Warrant, Search Warrant, Criminal Cover Sheet, this Motion to Seal, and any resulting Order be sealed for a period of one year or until the further Order of the Court, excepting the United States Attorney's Office and Law Enforcement Personnel, which may obtain copies of any of the foregoing documents or other sealed document for purposes of executing the Search Warrant, for the reason that the integrity of the ongoing investigation might be compromised should knowledge of the Search Warrant become public.

Executed June 8, 2023.

Respectfully submitted,

MARKENZY LAPOINTE  
UNITED STATES ATTORNEY

By:



Kiran N. Bhat  
Assistant United States Attorney  
Florida Bar No. 1008370  
99 NE 4th Street, 4th Floor  
Miami, Florida 33132  
Tel: (305) 961-9103  
kiran.bhat@usdoj.gov

FILED BY SM D.C.

**Jun 9, 2023**

ANGELA E. NOBLE  
CLERK U.S. DIST. CT.  
S. D. OF FLA. - FTL

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 23-MJ-6256-PAB

IN RE: SEALED SEARCH WARRANT  
\_\_\_\_\_

SEALING ORDER

**THIS CAUSE** is before the Court on the Government's Motion to Seal. Being fully advised, it is hereby **ORDERED AND ADJUDGED** that the motion is **GRANTED** and the following be **SEALED** for one year from the date of this order or until further order of the Court, whichever is sooner, excepting the United States Attorney's Office and Law Enforcement Personnel:

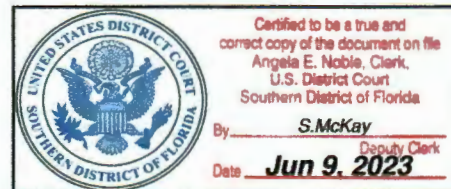
1. Application and Affidavit for Search Warrant dated June 9th, 2023;
2. Attachments to the Application and Search Warrant;
3. Search Warrant dated June 9th, 2023;
4. Criminal Cover Sheet;
5. This Sealing Order.

**DONE AND ORDERED** in Fort Lauderdale, Florida, this 9th day of June, 2023.



HON. PANAYOTTA AUGUSTIN-BIRCH  
UNITED STATES MAGISTRATE JUDGE

cc: AUSA Kiran N. Bhat





AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

## UNITED STATES DISTRICT COURT

for the  
Southern District of FloridaFILED BY SM D.C.

Jun 9, 2023

ANGELA E. NOBLE  
CLERK U.S. DIST. CT.  
S. D. OF FLA. - FTL

## In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)THE PREMISES LOCATED AT 9600 WEST SAMPLE ROAD,  
CORAL SPRINGS, FLORIDA, SUITES 100, 208, AND 300,  
AND ALL ELECTRONIC DEVICES THEREIN

Case No. 23-MJ-6256-PAB

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

located in the SOUTHERN District of FLORIDA, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section  
18 U.S.C. §§ 1349/1343  
18 U.S.C. §§ 1956/1957

Offense Description  
WIRE FRAUD CONSPIRACY/WIRE FRAUD  
MONEY LAUNDERING CONSPIRACY/MONEY LAUNDERING/ENGAGING IN  
TRANSACTIONS IN UNLAWFUL PROCEEDS

The application is based on these facts:

SEE ATTACHED AFFIDAVIT.

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under  
18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet



Certified to be a true and  
correct copy of the document on file  
Angela E. Noble, Clerk,  
U.S. District Court  
Southern District of Florida

By S. McKay Deputy Clerk  
Date Jun 9, 2023

Applicant's signature

SA AUSTIN STEELMAN, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
FACETIME (specify reliable electronic means).

Date: 6/9/2023

Judge's signature

City and state: FORT LAUDERDALE, FLORIDA

HON. PANAYOTTA AUGUSTIN-BIRCH, U.S. MAGISTRATE JUDGE

Printed name and title

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 23-MJ-6256-PAB

IN RE: THE SEARCH OF THE PREMISES  
LOCATED AT 9600 WEST SAMPLE ROAD,  
CORAL SPRINGS, FLORIDA, SUITES  
100, 208, AND 300, AND ALL ELECTRONIC  
DEVICES THEREIN

---

FILED BY SM D.C.

**Jun 9, 2023**

ANGELA E. NOBLE  
CLERK U.S. DIST. CT.  
S. D. OF FLA. - FTL

**SEALED AFFIDAVIT IN SUPPORT OF  
APPLICATION FOR SEARCH WARRANT**

I, Austin Steelman, being duly sworn, hereby depose and state as follows:

**INTRODUCTION**

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since February 2016. By virtue of my FBI employment, I am a law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7). I am currently assigned to the FBI Miami Field Office, Corporate and Securities Fraud Squad, which has investigative responsibility for fraud-related matters, including violations of the federal wire fraud and money laundering statutes. During my service as a Special Agent, I have managed and participated in many white-collar criminal investigations into *Ponzi* schemes, schemes related to corporate fraud and embezzlement, securities fraud, cryptocurrency fraud, and market manipulation. As part of this experience, I have sworn and executed many search warrants. I have also received related training and have learned through experience the methods and tactics used by white collar subjects to solicit, misappropriate, and obfuscate the use of investor funds. Before becoming an FBI Special Agent, I practiced law in Missouri, where I remain a member of the Bar on inactive status.



2. I make this Affidavit in support of an application for a warrant to search the office headquarters of Royal Bengal Logistics, Inc. ("RBL"), located at 9600 West Sample Road, Coral Springs, Florida, Suites 100, 208, and 300, and all electronic devices therein that reasonably appear to belong to Royal Bengal Logistics, Inc. or to persons working for Royal Bengal Logistics, Inc. (the "TARGET PREMISES"). The property to be searched is described in the following paragraphs and in Attachment A. The records and information to be seized are described in the following paragraphs and in Attachment B.

3. Based on the facts in this Affidavit, there is probable cause that Sanjay Singh ("SINGH") and others are operating an ongoing *Ponzi* scheme through RBL in violation of Title 18, United States Code, Sections 1349 (wire fraud conspiracy), 1343 (wire fraud), 1956(h) (money laundering conspiracy), and 1956(a)/1957 (money laundering) (the "Target Offenses"). There is also probable cause to search the TARGET PREMISES for evidence, instrumentalities, contraband, and fruits of these crimes.

4. The facts set forth in this Affidavit are based on my participation in the investigation; information and documents obtained from other law enforcement officers, other agencies, witnesses, and other persons; and knowledge gained from my training and experience. Because I am swearing this Affidavit for the limited purpose of establishing probable cause for a search warrant, this Affidavit does not include all facts that I have learned during this investigation.

5. This Court has jurisdiction to issue the requested warrant pursuant to Rule 41(b)(1), as the property to be searched and seized is located physically within this District.

## PROBABLE CAUSE

### *General Overview*

6. A “*Ponzi* scheme” is a fraud scheme that involves payment to existing investors from funds contributed by new investors. *Ponzi* scheme organizers often solicit investments by promising to use funds to pursue some legitimate business opportunity that generates high returns with little or no risk. Although *Ponzi* scheme organizers sometimes operate a real business to maintain a veneer of legitimacy, they focus primarily on attracting new investment fast enough to provide promised returns to existing investors. This creates the false appearance that the business is profitable, which inspires more new investment. Because success relies on attracting enough investment, however, *Ponzi* schemes collapse when new investment drops or when too many existing investors demand money back at once.

7. RBL, an over-the-road trucking company with corporate offices at the TARGET PREMISES in Coral Springs, is the vehicle for an ongoing *Ponzi* scheme that began in or around January 2020. From in and around February 2020 through in and around February 2023, RBL solicited over \$100 million from over 1,300 investors across 14 states and Haiti by promising guaranteed high returns. The investors were primarily individuals of Haitian descent, or companies controlled by individuals of Haitian descent. The initial investments were usually several tens of thousands of dollars. Financial analysis of RBL-related bank records and the statements of RBL’s own executives show that RBL did not have enough operating revenue to cover obligations to investors and instead routinely paid existing investors from new investor funds. SINGH also siphoned millions in investor funds to pay for home renovations, mortgage payments, personal expenses, and leveraged stock trades.



8. As its initial method to recruit new investors, RBL promised, typically through written contracts, to use an investor's funds to acquire a truck and/or trailer; to operate that equipment for about five years while making guaranteed monthly payments to the investor; and to provide title to the equipment to the investor at the end of the five-year period. RBL also guaranteed the investor's initial investment. In or around February 2023, however, RBL reported to its safety regulator, the Federal Motor Carrier Safety Administration ("FMCSA"), that it operated fewer trucks and trailers than it would likely have needed to keep all these promises. RBL also made other promises to raise new investment that dispensed with the trucking pretense altogether: For example, RBL pitched investors on a short-term investment program promising a return of 20 to 25 percent within a year or less.

9. The TARGET PREMISES is at the center of the RBL *Ponzi* scheme. RBL released a YouTube video in or around March 2023 featuring SINGH and others on site at the TARGET PREMISES. This video touted RBL's investment programs to the public. Moreover, RBL representatives have made misrepresentations at the TARGET PREMISES to both investors and undercover agents posing as potential investors. Undercover agents have observed multiple RBL personnel using computers at the TARGET PREMISES to conduct RBL business, including investment-related business tied to the *Ponzi* scheme. Internet Protocol ("IP") address analysis shows online access to bank accounts RBL has used to facilitate the *Ponzi* scheme from the Internet connection registered to the TARGET PREMISES. Further, the TARGET PREMISES also contains investor files and records of RBL's trucking activity relevant to establishing the falsity of RBL's representations regarding the trucking operation's scope and scale. Consequently, the TARGET PREMISES is likely to contain significant evidence, instrumentalities, contraband, or fruits of the Target Offenses.

*Relevant People and Entities*

10. Per Florida corporate records, RBL is a Florida corporation established on or about June 8, 2018, and headquartered at Suite 100 of the TARGET PREMISES. RBL maintains a website at rbl-inc.com, on which it lists its Department of Transportation registration number and describes itself as involved in “Long Haul Transportation” with offices at the TARGET PREMISES. Undercover agents posing as potential investors traveled to the TARGET PREMISES on March 17 and 31, 2023, and April 25, 2023, and confirmed that RBL operates at Suites 100, 208, and 300 of the TARGET PREMISES. Executive suites are located on the first floor, a dispatch operation is located on the second floor, and RBL investor relations are located on the third floor. Further surveillance confirmed RBL was using Suites 100, 208 and 300 at the TARGET PREMISES as of on or about June 2, 2023. The building in which the TARGET PREMISES is located is five stories tall and houses various other businesses. The requested warrant would authorize only a search of RBL-controlled areas.

11. SINGH, a resident of Coral Springs, is RBL’s President and Director and is a signer on each of RBL’s corporate bank accounts. Co-Conspirator 1, a resident of Coconut Creek, is RBL’s Vice President of Business Development and has solicited numerous investors. Co-Conspirator 2, a resident of Coral Springs, and Co-Conspirator 3, a resident of Riverview, are RBL’s Executive Directors of Business Development and solicit investors. Co-Conspirator 4, a resident of West Palm Beach, is RBL’s Executive Director of Investor Relations and serves as a self-described “bridge” between investors and RBL. Co-Conspirator 5, a resident of Parkland, is a Florida-barred attorney who is RBL’s General Counsel and Chief Compliance Officer. Co-Conspirator 6, a resident of Texas, is RBL’s co-founder and



Vice President of Credit & Acquisition and is a signer along with SINGH on certain corporate financial accounts. Co-Conspirator 7, a resident of Coral Springs, is SINGH's wife and RBL's Director of Finance. Co-Conspirator 8 is a former RBL employee and was a co-signer on certain RBL bank accounts with SINGH.

*Representations to the Public on YouTube*

12. RBL maintains a public YouTube channel<sup>1</sup> titled "Royal Bengal Logistics, INC. Administration" (the "RBL Channel") through which RBL's leadership team releases videos discussing, among other things, the company's operations and opportunities for investment. The RBL Channel is registered to an email address SINGH used to communicate with investors and subscriber records for the RBL Channel included payment mechanisms tied to SINGH. I preserved and reviewed the videos on the RBL Channel discussed below.

13. In a video titled "Driving American Dream," released through the RBL Channel in or around March 2023, SINGH walked into the offices at the TARGET PREMISES. He presented himself as the "founder and President" of RBL, a long-haul trucking and logistics company. He claimed "our business is to work for our investor, unlike other investment programs" and that "we take the risk, we take the liability, you enjoy the investment." SINGH further distinguished RBL from the "thousands of trucking companies" currently operating by saying RBL offers a "reverse franchisee model" in which investors can earn a "350% [] return of their initial capital." SINGH touted investments in RBL's "truck program," whereby RBL would use investor capital to purchase a truck, make loan payments on the truck for the investor, and provide the investor a monthly payment as well. According

---

<sup>1</sup> [https://www.youtube.com/channel/UC\\_LqPoL0JCVO7bSWKWey8XA](https://www.youtube.com/channel/UC_LqPoL0JCVO7bSWKWey8XA) (last accessed June 7, 2023).

to SINGH, once the truck loan was paid off, the investor would purportedly own the truck free and clear of any loans. SINGH boasted about the company's creation of "million-dollar companies" for its investors and concluded the video by stating: "I foresee this business to grow to 10 million investors in next 10 years." The video also repeatedly featured an overlay reading "Investment Opportunities 1200+ Clients."

14. In this same video, Co-Conspirator 3 appeared and described himself as one of the first four employees of the company and stated that he worked across all phases of the company, from talking to investors through getting a truck and hiring a driver. Co-Conspirator 4 appeared and described himself as a "bridge between RBL and investors." Co-Conspirator 6 appeared and stated that he has known SINGH since 2007 and co-founded RBL with SINGH. Co-Conspirator 1 appeared, described himself as the Vice President of Business Development, and stated that he has the "responsibility to make sure that the company just keeps on growing." Co-Conspirator 5 appeared and described her responsibilities as including trial litigation, dealing with outside law firms, preparing contracts, and giving the company legal advice. Co-Conspirator 5 stated that she had "observed and seen, uh, how effectively, [RBL has] been able to essentially grow with, you know, this investor system, it's a very unique system, and it allows us to grow very quickly and also, you know, survive, some of these industry-wide issues like gas." Co-Conspirator 2 appeared and stated that her responsibilities include working with investors, particularly out-of-state investors, "through email and phone calls."

15. In a video titled "ROYAL BENGAL LOGISTICS Investor Presentation," released through the RBL Channel in or around September 2022, Co-Conspirator 2 described



three distinct vehicles for potential RBL investors to achieve high returns while taking little risk.

16. The first was the primary “Equipment Management Investment” or “truck” program which “presents an opportunity to become a part of [RBL’s] business by owning a truck and gain assured monthly returns on your investment for a period of 58 months[.]” According to Co-Conspirator 2, an investor at that time could invest in one truck for \$45,000, and receive a monthly return of \$2,750 for 58 months, equating to \$159,500 in monthly payments total. Discounting the investor’s original principal of \$45,000, this means an investor would receive a return of approximately 254 percent over the investment period, not including the value of the truck.

17. The second was a “Short Term Attractive Return” investment, in which RBL provided the investor a “unique opportunity to multiply your income” and which “has the capability to offer [investors] handsome returns in a short period of time.” Through this program, an investor could provide a flat deposit and receive an up to 28 percent return after a certain number of days. For example, an investor could deposit \$50,000 and receive \$64,000 back after 180 days, a return of approximately 28 percent.

18. The third was a “Trailer Sponsorship Program” which allowed investors to provide funds for RBL to expand its “trailer manufacturing program.” According to Co-Conspirator 2, this program was a “sponsorship program for Royal Bengal to build and then resell a [tractor] trailer.” At the end of a six-month term, an investor would receive a profit of approximately 33 percent. For example, an investor may sponsor a trailer for \$45,000, and after 180 days receive \$60,000 back, including \$15,000 in profit.

*Representations to Investors at the TARGET PREMISES and Through Electronic Communication*

19. I interviewed B.E. as part of the investigation. B.E. invested in RBL's main truck program in or around April 2022. B.E. made an appointment with RBL and went to Suite 100 of the TARGET PREMISES, where the investment was described to him by an RBL representative. The RBL representative told B.E. his investment funds would be used to purchase two trucks; that RBL would register and deal with any licenses and registration for the trucks; that RBL would lease the trucks back from B.E.; and that RBL would make interest payments to B.E. starting two months after B.E. invested, even if a truck had not yet been acquired. B.E. understood his investment funds would be used to purchase trucks.

20. B.E. then sent RBL \$70,000 with the intention of having RBL purchase and operate two trucks for him while he received the promised monthly payments. B.E. signed a contract RBL provided him to memorialize this investment. The contract appeared drafted by an attorney in that it had integration, severability, *force majeure*, and other contractual clauses drafted specifically for the RBL truck program. B.E. ultimately demanded and received the initial investment back from RBL after RBL failed to make promised monthly payments to his satisfaction.

21. On or about March 17, 2023, an undercover employee of the FBI ("UCE-1") posed as a potential investor and went to the TARGET PREMISES to discuss a potential investment with RBL representatives. RBL staff directed UCE-1 to Suite 300 of the TARGET PREMISES on the third floor, where UCE-1 made a covert video and audio recording of the meeting with Co-Conspirator 2 and later Co-Conspirator 1.

22. Co-Conspirator 2 explained that RBL had started in 2018 and that the investment program began in 2019. She explained that there were over 1,000 investors in



RBL's main trucking program and "a bunch more" in the short-term investment program. Co-Conspirator 2 declined to provide UCE-1 with any of RBL's financial statements upon request, stating "we don't share financial information." Co-Conspirator 2 presented three potential RBL investment vehicles to UCE-1, which were similar to the three options Co-Conspirator 2 described in the September 2022 YouTube video discussed above, with the exceptions that potential initial investments were for different amounts and the "Trailer Sponsorship Program" had been replaced by replaced by a "Long Term Owner Financing" program through which RBL offered investors "long term financing with steady and secure returns at the maturity of the plan" without reference to trucks or trailers.

23. Co-Conspirator 2 explained that if UCE-1 invested \$55,000 with RBL, RBL would acquire UCE-1 a truck and would, over a 60-month period, pay UCE-1 \$174,000 total in "guaranteed monthly payment[s]," equating to a return of approximately 216 percent. Co-Conspirator 2 said that these payments would start two months after the initial investment, regardless of whether RBL had acquired a truck for UCE-1, which Co-Conspirator 2 said would take 9 to 12 months. Co-Conspirator 2 confirmed, "We here at RBL don't make any money off your \$55,000 or \$110,000 [initial payment] . . . . We only make money once we actually purchase your vehicle and start operating it." Co-Conspirator 2 gave assurances that UCE-1 would not lose the initial investment because of contractual protections and that even if RBL did not acquire UCE-1's truck, UCE-1 would receive the initial investment back. As a further benefit, at the end of the 60-month term, UCE-1 would receive a fully paid-for truck, titled under UCE-1's name. Co-Conspirator 2 also confirmed that RBL would help obtain financing for UCE-1's truck, that making loan payments would be RBL's responsibility, and

that RBL would provide a supplemental payment to UCE-1 for any loan payment UCE-1 made for the truck, above and beyond the “guaranteed monthly payment[s]” RBL promised.

24. When UCE-1 asked about the possibility of a short-term investment, Co-Conspirator 2 explained that UCE-1 could invest as little as \$25,000 and receive \$30,000 back after three months, equating to a 20 percent return. When UCE-1 asked about the “Trailer Sponsorship Program” that Co-Conspirator 2 described in the September 2022 YouTube video, Co-Conspirator 2 stated UCE-1 could sponsor RBL’s manufacture of its own trailers with parts from India. UCE-1 could invest \$50,000 for a six-month period and receive a “guaranteed payout at the end of the six months of \$65,000.” This equates to a 30 percent return.

25. As UCE-1 was speaking to Co-Conspirator 2, Co-Conspirator 1 approached and reiterated that UCE-1 would begin receiving the guaranteed monthly payments regardless of whether RBL had been able to obtain UCE-1’s truck. Immediately after the undercover meeting on or about March 17, 2023, the FBI surveillance team providing security for UCE-1 identified a black vehicle in the parking lot of the TARGET PREMISES registered to SINGH.

26. On or about March 31, 2023, UCE-1 again traveled to Suite 300 of the TARGET PREMISES along with an additional FBI undercover employee (“UCE-2”) posing as a second potential investor. UCE-1 and UCE-2 produced another covert video and audio recording of the meeting with Co-Conspirator 2.

27. Co-Conspirator 2 again went over the parameters of a potential investment, this time with UCE-2. When UCE-2 asked about the safety of the initial investment in RBL’s primary program, Co-Conspirator 2 responded that the equipment investment is “100 percent



guaranteed regardless of, if we're able to sell it, if we decide to use it ourselves, whatever the case may be, um, because that's RBL's responsibility at that point, all you're doing is just sponsoring us to use the funds . . . ." Co-Conspirator 2 also explained, "we don't solely rely on investors or investor income to, um, operate" and that RBL has "a fleet of our own vehicles." Co-Conspirator 2 claimed that RBL had 230 trucks purchased and 60 more "on our pipeline." Co-Conspirator 2 also explained that RBL accepts wires or cashier's checks from investors, and that she handled RBL's out-of-state investors. Co-Conspirator 2 also confirmed that RBL controlled the first and third floors of the TARGET PREMISES and that RBL had a suite on the second floor, which also housed an advertising company.

28. On or about April 25, 2023, UCE-2 again traveled to Suite 300 of the TARGET PREMISES posing as a potential investor. UCE-2 produced another covert video and audio recording including a meeting with Co-Conspirator 1 and a brief meeting with both Co-Conspirator 1 and SINGH. UCE-2 told Co-Conspirator 1 that the reason for the visit was to meet with the "people who run the business" including Co-Conspirator 1 and SINGH, to which Co-Conspirator 1 responded "yes, sir." Co-Conspirator 1 later described SINGH as the "president" and himself as the "vice president." Co-Conspirator 1 directed UCE-2 to "YouTube" where he said RBL "posts a bunch of stuff" about the company. Co-Conspirator 1 showed UCE-2 multiple RBL-related items on Co-Conspirator 1's computer. Co-Conspirator 1 explained that RBL is exclusively responsible for selecting an investor's truck under the truck program, advised that RBL tries to keep investor expectations for the quality of the trucks low while selecting the best trucks possible, and represented that "the business for us is the truck." Co-Conspirator 1 told UCE-2 "you get your payment no matter what" happens to the truck business and that no investors have ever missed payments. Co-

Conspirator 1 confirmed the layout of the TARGET PREMISES. Towards the end of the conversation, Co-Conspirator 1 fielded a telephone call from SINGH in UCE-2's presence during which SINGH explained that an investor was causing trouble and that RBL should terminate its relationship with this investor.

29. After meeting UCE-2 in Suite 300 of the TARGET PREMISES, Co-Conspirator 1 took UCE-2 to meet SINGH briefly in Suite 100 of the TARGET PREMISES. UCE-2 explained to SINGH that UCE-2 wanted to meet the person who built RBL. SINGH explained that each investor is a "pillar of the company" and that "you cannot be softened and weakened and become a loose pillar. . . people think they give us money and they are hands free. Hands free yes, but mentally you are there to help." SINGH explained that RBL tries to work with investors to give money back if needed, citing an example of an investor who died three months into the investment to whom RBL returned money "with interest." SINGH also explained that RBL is "running a truck" with the investment and that "99 percent of the time we will do our best, you will get everything you need."

30. During the meetings occurring on or about March 31 and April 25, 2023, at the TARGET PREMISES, UCE-1 and UCE-2 captured images of RBL representatives including SINGH, Co-Conspirator 1, and Co-Conspirator 2 using electronic devices to conduct RBL business:





*FMCSA Site Visit at the TARGET PREMISES and Subsequent Communication*

31. In or around February 2023, a safety investigator from the FMCSA, an agency within the United States Department of Transportation that regulates interstate trucking companies, visited the RBL offices at Suites 100 and 208 of the TARGET PREMISES as part of a normal safety inspection.

32. On or around February 28, 2023, the safety investigator entered Suite 100, where he observed Co-Conspirator 5's office immediately on the left upon entry into Suite 100, as well as SINGH's office within the same suite. The front door of Suite 100 had a paper attached to it directing investors to the third floor of the TARGET PREMISES. The safety investigator also traveled to the second floor, Suite 208, which he described as RBL's logistics management area for its trucks.

33. The safety investigator spoke with Co-Conspirator 5 and SINGH to discuss RBL's operations and safety compliance for its trucks, among other things. During these verbal discussions, and in follow-up written communications, Co-Conspirator 5 and SINGH told the safety investigator that RBL had approximately 119 trucks that it owned or leased, and that it had approximately 31 trailers that it owned or leased.

34. In a letter dated on or about February 23, 2023, Co-Conspirator 5 advised the safety investigator that RBL's estimated gross revenue for 2022 was \$7,848,712. Co-Conspirator 5 also advised in an email dated on or about February 24, 2023, that "RBL's financial condition is excellent, in the sense that its financial condition is in no way an impediment to the safe operation as an [over-the-road] carrier. RBL is well-capitalized. RBL's revenue and capital are more than enough to operate without 'cutting corners' and can absorb



significant losses without affecting those operations.” Co-Conspirator 5 also stated she was handling RBL’s safety program after the departure of another employee on February 15, 2023.

*Financial Analysis*

35. Law enforcement obtained and reviewed records corresponding to approximately 80 bank and brokerage accounts related to RBL and its executives. Investigators focused in particular on three accounts held in RBL’s name which, when open, appear to have been the company’s primary operating accounts into which investor money flowed and out of which RBL paid investors: (1) an account open from in or around October 2019 through September 2022 at Bank of America ending in 6001 (“BOA 6001”); (2) an account open from in or around October 2021 through in or around July 2022 at Citibank ending in 4380 (“Citi 4380”); and (3) an account open at Wells Fargo Bank from in or around May 2021 through the present ending in 5094 (“WF 5094”). In or around November 11, 2022, Co-Conspirator 2 made public statements in a video posted to the RBL channel stating that RBL was no longer accepting wires to the company’s Bank of America account and instead was accepting wires to the company’s Wells Fargo account, consistent with what law enforcement observed in patterns of use for these accounts.

36. Financial analysis of RBL’s three primary operating accounts, BOA 6001, Citi 4380, and WF 5094, confirmed RBL’s public representations that it obtained investments from over 1,000 investors. These investments totaled more than \$100 million. RBL’s investors typically sent RBL upfront payments (e.g., by wire transfers, cashier’s check, etc.) worth tens of thousands of dollars each. RBL then regularly paid existing investors back a percentage of that principal on a month-to-month basis, typically through automated clearinghouse (“ACH”) payments. This pattern continued through the most recent records for what the

government understands to be the only remaining active RBL operating account, WF 5094, dated May 2023.

37. Because RBL pays over 1,000 investors thousands of dollars each month and has promised to provide returns on the more than \$100 million it has taken in from investors, RBL has incurred well over \$100 million in total obligations to investors since beginning its investment programs in and around February 2020. Law enforcement estimates that as of February 2023, RBL had paid out about \$62 million to investors. Yet during the same timeframe, from in and around February 2020 to in and around February 2023, law enforcement estimates from RBL's bank records that RBL had revenues from trucking of only about \$16 million, against operating costs over \$30 million. In other words, RBL's trucking business was losing money, requiring RBL to pay existing investors from new investor funds.

38. Corroborating this review as to revenue, Co-Conspirator 5 stated to FMCSA on or about February 23, 2023, that RBL had approximately \$7,848,712 in 2022 revenue. Conservatively assuming RBL had the same revenue in 2020 and 2021, RBL would have had approximately \$24 million in revenue since the inception of the company's investment programs in or around February 2020. Although law enforcement's review of the bank records suggest that the true revenue figure is less, even \$24 million in revenue from 2019 through 2022 would not be sufficient to support the guaranteed returns RBL promised investors in addition to RBL's expenses.

39. Illustrating this point, based on review of bank records from WF 5094, from in and around October 2022 to January 2023, RBL paid out approximately \$22 million to previous investors. By RBL's own report—Co-Conspirator 5's statement to FMCSA on or about February 23, 2023, that RBL had approximately \$7,848,712 in 2022 revenue—RBL did



not make enough trucking revenue in all of 2022 to cover just four months of payouts it recently made to investors. This is not factoring in records from Automatic Data Processing, Inc., a payroll company, which show that RBL spent approximately \$6 million alone in 2022 to cover a single expense: its payroll-related liabilities.

40. Based on all the evidence gathered to date, RBL does not disclose to potential investors that its continued existence is dependent on new investment. Instead, RBL gives investors the impression that their guaranteed returns arise from RBL's business operations involving the trucks that RBL is helping investors obtain. RBL even projected the same impression to a regulator. Co-Conspirator 5 recently characterized RBL as in "excellent" financial condition and "well-capitalized" to FMSCA officials in or around February 2023. And although Co-Conspirator 5 indicated this statement was based on RBL's "revenue and capital[.]" RBL's obligations to its investors will outweigh available "capital"—i.e., funds from new investors—as soon as new investment falls. Thus, based on the financial analysis in this section, the recorded conversations with UCE-1 and UCE-2, investor materials and public promotional materials obtained from RBL, and interviews with investors, law enforcement believes that RBL is operating a *Ponzi* scheme in which it pays existing investors with new investor funds.

*Misappropriation of Investor Funds*

41. Contrary to Co-Conspirator 2's representation to UCE-1 that "we here at RBL don't make any money off your \$55,000 or \$110,000 [initial payment]," law enforcement's review of RBL-related bank records shows that SINGH diverted tens of millions of dollars of investor funds that were not used to acquire trucks or trailers for investors as promised.



42. From the three RBL operating accounts described above, approximately \$12 million went to SINGH's personal brokerage account. Trading activity from SINGH's personal brokerage account showed that SINGH used investor funds to trade various stocks on margin, often at a loss. SINGH also transferred about \$8 million from his personal brokerage account to RBL's operating accounts. Likewise, from RBL's three primary operating accounts, approximately \$16 million went to a brokerage account titled to RBL, where SINGH also engaged in leveraged stock trading activity. SINGH also transferred about \$8 million back from this RBL brokerage account into RBL's operating accounts. In total, law enforcement estimates that SINGH diverted at least \$12 million in funds from RBL's primary operating accounts, which contained primarily investor funds intermingled to a lesser extent with business revenue, to these two brokerage accounts.

43. RBL's operating accounts also showed approximately \$1 million of spending on SINGH's personal expenses, including but not limited to mortgage payments on his residence, payments to family members, and restaurants.

*Electronic Devices Within the Target Premises Accessed Scheme Bank Accounts*

44. Based on my training and experience, I know that an Internet Service Provider ("ISP") typically assigns the Internet connection at a specific physical location an IP address and keeps subscriber records for the entity paying for that Internet connection. Any electronic device accessing a website or other Internet-based application from that physical location would display, in that website or application provider's Internet connection logs, the IP address that the ISP assigned to that Internet connection. Some banks keep Internet connection logs showing IP addresses that access online banking services for specific bank accounts. By cross-referencing these records, law enforcement can sometimes determine that

the Internet connection at a specific location was used to access a specific bank account. Law enforcement typically cannot, however, determine which electronic device within that location was used to access the specific bank account without access to the electronic devices themselves, as all electronic devices accessing the bank account from that location will display the same IP address.

45. I analyzed Internet connection logs from the BOA 6001 account and the WF 5094 account, as well as subscriber records associated with the Internet connection at the TARGET PREMISES, for which RBL was the registered subscriber. My analysis showed that an electronic device or electronic devices using the Internet connection at the TARGET PREMISES consistently accessed the BOA 6001 and the WF 5094 bank accounts to move funds in those accounts as part of the RBL *Ponzi* scheme.

46. For example, on or around March 31, 2022, someone with the online banking username “rbl3149658” used a device displaying an IP address assigned to the TARGET PREMISES to move \$250,000 from BOA 6001 to a bank account in the name of Co-Conspirator 7, SINGH’s wife. As a second example, on or around June 3, 2022, someone with the online banking username “sjay2020boa” used a device displaying an IP address assigned to the TARGET PREMISES to move \$250,000 from BOA 6001 to a brokerage account that was used to trade stocks and not for any business related to trucking. There were numerous other instances in 2022 in which devices displaying the IP address assigned to the TARGET PREMISES interacted with the BOA 6001 account via online banking.

47. Similarly, a review of WF 5094 records showed that devices displaying the IP address associated with the TARGET PREMISES interacted with online banking services for the WF 5094 account in 2022 and 2023.



48. In sum, people handling RBL's corporate bank accounts, likely including the account signer SINGH, and others, routinely accessed RBL's accounts using the Internet connection at the TARGET PREMISES. Some of these uses include misappropriation of large sums of investor funds that have no apparent relation to purchasing trucks or operating RBL's business.

*RBL Maintains Investor Files at the TARGET PREMISES*

49. I interviewed S.M., who worked at RBL from in or around February to July 2021. During his tenure, S.M. assisted with managing RBL's truck fleet. S.M. said that RBL could not keep its trucks running and struggled to maintain its credit. SINGH could never afford to fix RBL's trucks, and sometimes necessary repairs were not made before trucks were allowed back into operation. S.M. remembered when RBL management celebrated selling its "100th truck," meaning RBL had brought in 100 truck investors. S.M. noted, however, that at the time, the company only had approximately 38 trucks in operation. This did not make sense to S.M., who began to think that RBL might be a *Ponzi* scheme.

50. Approximately two weeks after S.M. started at RBL, S.M. observed approximately five men come into the RBL office. Three or four of the men were carrying duffel bags of cash. The cash was more money than S.M. had ever seen. The men carrying the duffel bags of cash went into Co-Conspirator 1's office, set the cash down, and Co-Conspirator 1 said, "Oh, it's payday!" and high-fived SINGH. Co-Conspirator 1 then said something to the effect of, "this is our investment."

51. During his tenure, S.M. observed that physical investor files were kept in a locked cabinet in Co-Conspirator 1's office on the first floor of the TARGET PREMISES.



*Probable Cause Exists to Search the TARGET PREMISES*

52. Based on the foregoing, I believe SINGH and others at RBL are engaged in a *Ponzi* scheme headquartered at the TARGET PREMISES. Documents and materials from the TARGET PREMISES, both electronic and physical, will help investigators establish that RBL does not generate sufficient revenues to service its debt to existing investors without bringing in new investors. Further, evidence from the TARGET PREMISES will help investigators account for and identify victims, show misappropriation of investor funds, and show correspondence between RBL's operators to establish knowledge of any underlying misrepresentations.

53. There is probable cause that evidence of a crime, or fruits thereof, are located within electronic devices at the TARGET PREMISES because electronic devices routinely connected to RBL's bank accounts used to perpetrate the scheme from the TARGET PREMISES's internet connection; because UCE-1 and UCE-2 observed RBL personnel using electronic devices to conduct RBL business and RBL investment pitches; because RBL uses email and other electronic correspondence to communicate with investors; because RBL uses electronic systems to run the trucking operation it maintains and to communicate with regulators about this business; because RBL has provided investors with pitch materials that appear to have been produced on an electronic device; and because of the ubiquity of electronic communications between those operating any business enterprise.

**BACKGROUND REGARDING SEARCH OF ELECTRONIC DEVICES**

54. I submit that if, as anticipated, a computer, cell phone, or storage medium is found at the TARGET PREMISES, there is probable cause to believe records will be stored on that computer, cell phone, or storage medium, for at least the following reasons:

a. Based upon my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

e. Based on actual inspection of other evidence related to this investigation, including documents submitted by RBL to FMCSA and sent by RBL to investors, I



am aware that computer equipment was used to generate and store documents and data used in the scheme.

55. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium at the TARGET PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my



training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpatory or exculpatory the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the

computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.



56. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements.* Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the



system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

57. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including, but not limited to, computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

#### **FILTER PROCESS**

58. Although Co-Conspirator 5 is a Florida-barred attorney and serves as general counsel for RBL, based on the facts above, the government understands Co-Conspirator 5 to have been involved in RBL's operations and to have performed business functions in addition to legal functions. Co-Conspirator 5 is currently managing RBL's "safety program" as of February 2023 and has made statements regarding the financial viability of the company to FMCSA. Co-Conspirator 5 listed herself on LinkedIn as RBL's Chief Executive Officer as of in or around May 2023. Materials from Co-Conspirator 5's office will likely show that she knew that RBL is not financially viable absent new investment and is instead a *Ponzi* scheme.

59. Additionally, law enforcement understands that at minimum, Co-Conspirator 5 has allowed RBL to use her legal services in furtherance of the scheme described above. For

instance, Co-Conspirator 5 filed a lawsuit for RBL in federal court against Citibank after, in or around July 2022, Citibank froze about \$1.5 million then in Citi 4380 on suspicion of fraud.

*See Royal Bengal Logistics, Inc. v. Citibank, N.A.*, Case No. 22-cv-61050, DE 1 (S.D. Fla. June 2, 2022). The complaint Co-Conspirator 5 signed stated on behalf of RBL that the “funds in [Citi 4380] are not the proceeds of fraudulent or illegal activity” and that RBL needed “the funds that have been wrongfully seized by Citibank to pay Royal Bengal’s employees, investors, and creditors for obligations incurred in its business.” *Id.*

60. The United States Securities and Exchange Commission (“SEC”) may soon be initiating an action against RBL and SINGH in which the SEC will request that the Court appoint a receiver to manage RBL’s affairs. Contingent on the SEC not obtaining this Court-appointed receiver, law enforcement intends to search Co-Conspirator 5’s office within the TARGET PREMISES pursuant to the attorney office search filter procedure described further in Attachment B. Because concerns over the spoliation of evidence would be substantially mitigated if the SEC obtains a Court-appointed receiver, law enforcement will in that scenario cordon off Co-Conspirator 5’s office during the execution of the requested warrant, will not search Co-Conspirator 5’s office, and will seek to obtain relevant records from Co-Conspirator 5’s office pursuant to legal process to be served on RBL via the receiver, allowing the receiver to conduct the required privilege review.

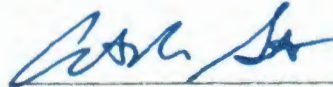
61. Regardless of whether the SEC obtains a Court-appointed receiver, law enforcement intends to submit all electronic devices and any physical materials seized pursuant to the requested search warrant through the evidentiary filter process described further in Attachment B. The purpose of this evidentiary filter review is to ensure that the case team is not exposed to any materials protected by attorney-client or work product privileges.



**CONCLUSION**

62. For the reasons above, there is probable cause to believe that SINGH and others have engaged in the Target Offenses and that evidence, fruits, and instrumentalities of these violations exist at the TARGET PREMISES. I therefore request that the Court issue the attached warrant.

Respectfully submitted,

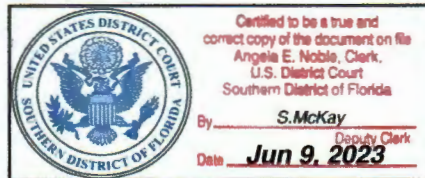


Special Agent Austin Steelman  
Federal Bureau of Investigation

Attested to me by the applicant in accordance with the requirements of Fed.R.Crim.P.4.1 by FaceTime this 9th day of June, 2023.



HONORABLE PANAYOTTA AUGUSTIN-BIRCH  
UNITED STATES MAGISTRATE JUDGE





**ATTACHMENT A**

**PROPERTY TO BE SEARCHED**

The premises to be searched are the offices of Royal Bengal Logistics, Inc., which occupy Suites 100, 208, and 300 at 9600 West Sample Road, Coral Springs, Florida, and all electronic devices therein that reasonably appear to belong to Royal Bengal Logistics, Inc. or to persons working for Royal Bengal Logistics, Inc. The premises includes offices on the ground floor, the second floor, and the third floor of a five-story office building. Pictures of the premises are below.







## **ATTACHMENT B**

### **ITEMS TO BE SEIZED**

All documents and records<sup>2</sup> that are evidence, fruits, or instrumentalities related to violations of Title 18, United States Code, Sections 1343 (wire fraud), 1349 (conspiracy to commit mail fraud and wire fraud), 1956 (money laundering and money laundering conspiracy) and 1957 (engaging in transactions in unlawful proceeds), occurring from January 2020 through the date of the warrant and committed by Sanjay Singh and co-conspirators, specifically, the following:

1. Investment related documents and records such as equipment management agreements, short-term and long-term financing agreements, trailer sponsorship agreements, interest payment schedules, investor questionnaires, and any other investment agreements or files;
2. Documents and records related to investors and possible investors, including lists and documents containing names, identifying information, financial or credit worth profiles, account numbers, telephone numbers, e-mail addresses, bank account numbers;
3. Documents and records related to soliciting investors, including records of conversations, notes, offering materials, sales scripts, marketing materials, correspondence,<sup>3</sup> lead lists, journals, or telephone messages;
4. Documents and records reflecting correspondence and communications between Sanjay Singh and co-conspirators, or between investors and Sanjay Singh and his co-conspirators;
5. Documents and records related to long-haul truck operations, including profit and loss statements, financial statements, leases, purchase agreements, operational records, maintenance records, loan records, contracts with factoring companies, safety records, correspondence with or submission to regulators, and payroll or independent contractor payment records;
6. Documents and records filed with secretaries of state offices, such as Florida Sunbiz records;

---

<sup>2</sup> The terms "documents" and "records" have their common meaning, including, but not limited to, writings, correspondence, lists, transcripts, handouts, agreements and contracts, recordings, spreadsheets, images, in whatever form and by whatever means they may exist, have been created or stored, including in electronic or digital form (such as any information on a computers, tablet devices, CD-ROMs, flash drives, optical discs, printer buffers, smart cards, servers, memory calculators, pagers, smart phones, as well as printouts or readouts from any magnetic storage device); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, slides, videotapes).

<sup>3</sup> The term "correspondence" has its common meaning and includes text messages, letters, electronic mail, mailings, and inter office messages and notes.



7. Documents and records filed and related to the filing of documents with regulatory bodies such as the Federal Motor Carrier Safety Administration, U.S. Securities and Exchange Commission ("SEC"), or state equivalents;
8. Documents and records evincing relationships with and between Royal Bengal Logistics, Inc. and other corporate entities;
9. Internal correspondence such as memoranda, meeting minutes or notes relevant to the other items on this list;
10. Recordings and images, including interior and exterior surveillance and pictures, depicting entry and exit of persons, and presence of persons inside the premises;
11. Accounting records such as profit and loss statements, balance sheets, and equity statements, or investor statements;
12. Documents related to financial transactions, such account statements, deposit and withdrawal slips, checks, money orders, wire memos, signature cards, account numbers, applications, bank cards and credit cards of Royal Bengal Logistics, Inc. and other entities, wire transfer requests or confirmations;
13. Receipts, invoices or other similar records showing the uses of investor funds and business expenses;
14. Employment records such as work schedules, applications, contracts, employee lists and contact information, employment handbooks, employment policies, timecards, payment of bonuses, commissions and salaries, and wage or earning statements;
15. Computer devices, including tablets, used for the business and investor solicitation;
16. FedEx, UPS, or USPS shipping labels, invoices, and tracking numbers;
17. Business documents or records such as articles of incorporation, articles of organization, operating agreements, membership lists, or organization charts;
18. Proceeds of investments and investors, including cash and bank checks;
19. Items of identification and papers, documents and effects which establish use, dominion and control of premises, or part of the premises, including, but not limited to, keys, mail, envelopes, bills from public utilities, photos, address books and similar items;
20. Cellular telephones that may reasonably contain any of the documents and records reflected above; and
21. For any computer, cell phone, or storage medium whose seizure is otherwise authorized by this warrant, and any computer, cell phone, or storage medium that contains or in which is stored records or information that are otherwise called for by this warrant (hereinafter, "COMPUTER");
  - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c. evidence of the lack of such malicious software;



- d. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the COMPUTER user;
  - e. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
  - f. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
  - g. evidence of the times the COMPUTER was used;
  - h. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
  - i. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
  - j. records of or information about Internet Protocol addresses used by the COMPUTER; and
  - k. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
22. Electronically stored information containing the information described above. The process for collecting such information is described below.

#### **ELECTRONICALLY STORED INFORMATION**

23. The above identified information and/or data may be stored in the form of magnetic or electronic coding on computer media, or on media capable of being read by a computer or with the aid of a computer related equipment. This media includes any magnetic or electronic storage device such as servers, floppy diskettes, hard disks, backup tapes, CD-ROMs, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, electronic notebooks, cellular telephones, smartphones (e.g., iPhone), or mobile media players (e.g., iPods and iPads). In searching for data capable of being read, stored or interpreted by a computer, law enforcement personnel executing this search warrant will employ the following procedure:
- a. Upon securing the premises, law enforcement personnel trained in searching and seizing computer data (the "computer personnel") may make an initial review of any computer equipment and storage devices to determine whether or not these items can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve the data.
  - b. If the computer equipment and storage devices cannot be searched on-site in a reasonable amount of time and without jeopardizing the preservation of the data, then the computer personnel will determine whether it is practical to copy/image the data.
  - c. If the computer personnel determine it is not practical to perform an on-site searching, copying or imaging (due to time, technical or other considerations), then the computer equipment and storage devices will be seized and transported to an appropriate law enforcement laboratory for review. The



computer equipment and storage devices will be reviewed by appropriately trained personnel to extract and seize any data that falls within the list of items to be seized set forth herein.

- d. Any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offense, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) any data that falls within the list of items to be seized set forth within.
- e. In searching the data, computer personnel may examine all of the data contained in the computer equipment and storage devices to view their precise contents and determine whether the data falls within the items to be seized as set forth herein.
- f. If the computer personnel determine that the computer equipment and storage devices are no longer necessary to retrieve and preserve the data, and the items are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(b), the government will return these items within a reasonable period of time.
- g. In order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel may need to seize and search the following items, subject to the procedures set forth above:
  - i. Any computer equipment and storage devices capable of being used to commit or store evidence of the offenses listed above;
  - ii. Any computer equipment used to facilitate the transmission, creation, display, encoding or storage of data, including but not limited to word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners;
  - iii. Any magnetic, electric or optical storage device capable of storing data such as servers, floppy disks, hard disk tapes, CD-ROMs, CDRs, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, USB flash memory devices, personal digital assistants, mobile telephones or answering machines;
  - iv. Any documentation, operating logs and reference manuals regarding the operation of the computer equipment, storage devices, or software;
  - v. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices or data to be searched;
  - vi. Any physical keys, encryption devices and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and
  - vii. Any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices.



### **FILTER PROCEDURES**

24. The following procedures will be followed at the time of the search in order to protect against disclosures of privileged or protected material.
25. These procedures will be executed by: (a) law enforcement personnel and other individuals assisting them who are not participating in the investigation of the matter who will conduct the search (the "Search Team"); and (b) separate law enforcement personnel and other individuals assisting them who are not participating in the investigation who will be available to assist in the event that a procedure involving potentially privileged information is required (the "Filter Team").
26. Contingent upon the absence of a Court-appointed receiver managing the affairs of Royal Bengal Logistics, Inc., the Filter Team will be responsible for segregating and searching the work area used by E.O.H. within the premises, or any other area of the premises that appears to be used by an attorney in furtherance of the practice of law. The Filter Team will also be permitted to search for and seize potentially privileged information responsive to this warrant contained in areas of the premises that are not in an area where an attorney conducts his or her work in the practice of law, subject to the privilege review outlined below. The Search Team will be responsible for searching all areas of the premises that appear not to be used by an attorney in furtherance of the practice of law, also subject to the privilege review outlined below. Should a Court-appointed receiver be managing the affairs of Royal Bengal Logistics, Inc., however, neither the Filter Team nor the Search Team shall search E.O.H.'s work area, or any other area of the premises that appears to be used by an attorney in furtherance of the practice of law.
27. After the execution of the search by the Search Team and, where necessary, the Filter Team, the Filter Team will review physical and electronic materials seized to identify and segregate documents or data containing potentially privileged information.
28. If the Filter Team determines the documents or data are not potentially privileged, they may be provided to the law enforcement personnel assigned to the investigation immediately. If at any point the law enforcement personnel assigned to the investigation subsequently identify any data or documents that they consider may be potentially privileged, they will cease the review of such identified data or documents and refer the materials to the Filter Team for further review by the Filter Team.
29. If the Filter Team determines that documents are potentially privileged or merit further consideration in that regard, a Filter Team attorney may do any of the following: (a) apply *ex parte* to the court for a determination whether or not the documents contain privileged material; (b) defer seeking court intervention and continue to keep the documents inaccessible to law enforcement personnel assigned to the investigation; or (c) disclose the documents to the potential privilege holder, request the privilege holder to state whether the potential privilege holder asserts privilege as to any documents, including requesting a particularized privilege log, and seek a ruling from the court regarding any privilege claims as to which the Privilege Review Team and the privilege-holder cannot reach agreement.



AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means

☐ Original☐ Duplicate Original

## UNITED STATES DISTRICT COURT

for the  
Southern District of FloridaFILED BY SM D.C.

Jun 9, 2023

ANGELA E. NOBLE  
CLERK U.S. DIST. CT.  
S. D. OF FLA. - FTL

In the Matter of the Search of )  
 (Briefly describe the property to be searched )  
 or identify the person by name and address) )  
 THE PREMISES LOCATED AT 9600 WEST SAMPLE )  
 ROAD, CORAL SPRINGS, FLORIDA, SUITES 100, 208, )  
 AND 300, AND ALL ELECTRONIC DEVICES THEREIN )

Case No. 23-MJ-

## WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

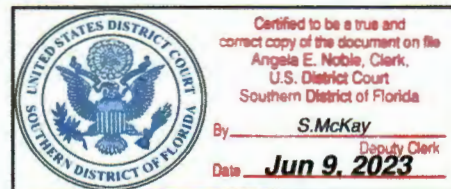
To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the SOUTHERN District of FLORIDA  
 (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

SEE ATTACHMENT B.



**YOU ARE COMMANDED** to execute this warrant on or before 6/23/2023 (not to exceed 14 days)  
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to \_\_\_\_\_  
 (United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for \_\_\_\_\_ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of \_\_\_\_\_

Date and time issued: 6/9/2023 1:45 p.m.

Judge's signature

City and state: FORT LAUDERDALE, FLORIDA

HON. PANAYOTTA AUGUSTIN-BIRCH, U.S. MAGISTRATE JUDGE  
 Printed name and title



Return		
Case No.: 23-MJ-6256-PAB	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:               		
Certification		
I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.		
Date: _____	_____ <i>Executing officer's signature</i>	
	_____ <i>Printed name and title</i>	

**ATTACHMENT A**

**PROPERTY TO BE SEARCHED**

The premises to be searched are the offices of Royal Bengal Logistics, Inc., which occupy Suites 100, 208, and 300 at 9600 West Sample Road, Coral Springs, Florida, and all electronic devices therein that reasonably appear to belong to Royal Bengal Logistics, Inc. or to persons working for Royal Bengal Logistics, Inc. The premises includes offices on the ground floor, the second floor, and the third floor of a five-story office building. Pictures of the premises are below.







## **ATTACHMENT B**

### **ITEMS TO BE SEIZED**

All documents and records<sup>2</sup> that are evidence, fruits, or instrumentalities related to violations of Title 18, United States Code, Sections 1343 (wire fraud), 1349 (conspiracy to commit mail fraud and wire fraud), 1956 (money laundering and money laundering conspiracy) and 1957 (engaging in transactions in unlawful proceeds), occurring from January 2020 through the date of the warrant and committed by Sanjay Singh and co-conspirators, specifically, the following:

1. Investment related documents and records such as equipment management agreements, short-term and long-term financing agreements, trailer sponsorship agreements, interest payment schedules, investor questionnaires, and any other investment agreements or files;
2. Documents and records related to investors and possible investors, including lists and documents containing names, identifying information, financial or credit worth profiles, account numbers, telephone numbers, e-mail addresses, bank account numbers;
3. Documents and records related to soliciting investors, including records of conversations, notes, offering materials, sales scripts, marketing materials, correspondence,<sup>3</sup> lead lists, journals, or telephone messages;
4. Documents and records reflecting correspondence and communications between Sanjay Singh and co-conspirators, or between investors and Sanjay Singh and his co-conspirators;
5. Documents and records related to long-haul truck operations, including profit and loss statements, financial statements, leases, purchase agreements, operational records, maintenance records, loan records, contracts with factoring companies, safety records, correspondence with or submission to regulators, and payroll or independent contractor payment records;
6. Documents and records filed with secretaries of state offices, such as Florida Sunbiz records;

---

<sup>2</sup> The terms "documents" and "records" have their common meaning, including, but not limited to, writings, correspondence, lists, transcripts, handouts, agreements and contracts, recordings, spreadsheets, images, in whatever form and by whatever means they may exist, have been created or stored, including in electronic or digital form (such as any information on a computers, tablet devices, CD-ROMs, flash drives, optical discs, printer buffers, smart cards, servers, memory calculators, pagers, smart phones, as well as printouts or readouts from any magnetic storage device); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, slides, videotapes).

<sup>3</sup> The term "correspondence" has its common meaning and includes text messages, letters, electronic mail, mailings, and inter office messages and notes.



7. Documents and records filed and related to the filing of documents with regulatory bodies such as the Federal Motor Carrier Safety Administration, U.S. Securities and Exchange Commission ("SEC"), or state equivalents;
8. Documents and records evincing relationships with and between Royal Bengal Logistics, Inc. and other corporate entities;
9. Internal correspondence such as memoranda, meeting minutes or notes relevant to the other items on this list;
10. Recordings and images, including interior and exterior surveillance and pictures, depicting entry and exit of persons, and presence of persons inside the premises;
11. Accounting records such as profit and loss statements, balance sheets, and equity statements, or investor statements;
12. Documents related to financial transactions, such account statements, deposit and withdrawal slips, checks, money orders, wire memos, signature cards, account numbers, applications, bank cards and credit cards of Royal Bengal Logistics, Inc. and other entities, wire transfer requests or confirmations;
13. Receipts, invoices or other similar records showing the uses of investor funds and business expenses;
14. Employment records such as work schedules, applications, contracts, employee lists and contact information, employment handbooks, employment policies, timecards, payment of bonuses, commissions and salaries, and wage or earning statements;
15. Computer devices, including tablets, used for the business and investor solicitation;
16. FedEx, UPS, or USPS shipping labels, invoices, and tracking numbers;
17. Business documents or records such as articles of incorporation, articles of organization, operating agreements, membership lists, or organization charts;
18. Proceeds of investments and investors, including cash and bank checks;
19. Items of identification and papers, documents and effects which establish use, dominion and control of premises, or part of the premises, including, but not limited to, keys, mail, envelopes, bills from public utilities, photos, address books and similar items;
20. Cellular telephones that may reasonably contain any of the documents and records reflected above; and
21. For any computer, cell phone, or storage medium whose seizure is otherwise authorized by this warrant, and any computer, cell phone, or storage medium that contains or in which is stored records or information that are otherwise called for by this warrant (hereinafter, "COMPUTER");
  - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c. evidence of the lack of such malicious software;



- d. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the COMPUTER user;
  - e. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
  - f. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
  - g. evidence of the times the COMPUTER was used;
  - h. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
  - i. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
  - j. records of or information about Internet Protocol addresses used by the COMPUTER; and
  - k. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
22. Electronically stored information containing the information described above. The process for collecting such information is described below.

#### **ELECTRONICALLY STORED INFORMATION**

23. The above identified information and/or data may be stored in the form of magnetic or electronic coding on computer media, or on media capable of being read by a computer or with the aid of a computer related equipment. This media includes any magnetic or electronic storage device such as servers, floppy diskettes, hard disks, backup tapes, CD-ROMs, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, electronic notebooks, cellular telephones, smartphones (e.g., iPhone), or mobile media players (e.g., iPods and iPads). In searching for data capable of being read, stored or interpreted by a computer, law enforcement personnel executing this search warrant will employ the following procedure:
- a. Upon securing the premises, law enforcement personnel trained in searching and seizing computer data (the "computer personnel") may make an initial review of any computer equipment and storage devices to determine whether or not these items can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve the data.
  - b. If the computer equipment and storage devices cannot be searched on-site in a reasonable amount of time and without jeopardizing the preservation of the data, then the computer personnel will determine whether it is practical to copy/image the data.
  - c. If the computer personnel determine it is not practical to perform an on-site searching, copying or imaging (due to time, technical or other considerations), then the computer equipment and storage devices will be seized and transported to an appropriate law enforcement laboratory for review. The



computer equipment and storage devices will be reviewed by appropriately trained personnel to extract and seize any data that falls within the list of items to be seized set forth herein.

- d. Any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offense, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) any data that falls within the list of items to be seized set forth within.
- e. In searching the data, computer personnel may examine all of the data contained in the computer equipment and storage devices to view their precise contents and determine whether the data falls within the items to be seized as set forth herein.
- f. If the computer personnel determine that the computer equipment and storage devices are no longer necessary to retrieve and preserve the data, and the items are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(b), the government will return these items within a reasonable period of time.
- g. In order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel may need to seize and search the following items, subject to the procedures set forth above:
  - i. Any computer equipment and storage devices capable of being used to commit or store evidence of the offenses listed above;
  - ii. Any computer equipment used to facilitate the transmission, creation, display, encoding or storage of data, including but not limited to word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners;
  - iii. Any magnetic, electric or optical storage device capable of storing data such as servers, floppy disks, hard disk tapes, CD-ROMs, CDRs, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, USB flash memory devices, personal digital assistants, mobile telephones or answering machines;
  - iv. Any documentation, operating logs and reference manuals regarding the operation of the computer equipment, storage devices, or software;
  - v. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices or data to be searched;
  - vi. Any physical keys, encryption devices and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and
  - vii. Any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices.



### **FILTER PROCEDURES**

24. The following procedures will be followed at the time of the search in order to protect against disclosures of privileged or protected material.
25. These procedures will be executed by: (a) law enforcement personnel and other individuals assisting them who are not participating in the investigation of the matter who will conduct the search (the "Search Team"); and (b) separate law enforcement personnel and other individuals assisting them who are not participating in the investigation who will be available to assist in the event that a procedure involving potentially privileged information is required (the "Filter Team").
26. Contingent upon the absence of a Court-appointed receiver managing the affairs of Royal Bengal Logistics, Inc., the Filter Team will be responsible for segregating and searching the work area used by E.O.H. within the premises, or any other area of the premises that appears to be used by an attorney in furtherance of the practice of law. The Filter Team will also be permitted to search for and seize potentially privileged information responsive to this warrant contained in areas of the premises that are not in an area where an attorney conducts his or her work in the practice of law, subject to the privilege review outlined below. The Search Team will be responsible for searching all areas of the premises that appear not to be used by an attorney in furtherance of the practice of law, also subject to the privilege review outlined below. Should a Court-appointed receiver be managing the affairs of Royal Bengal Logistics, Inc., however, neither the Filter Team nor the Search Team shall search E.O.H.'s work area, or any other area of the premises that appears to be used by an attorney in furtherance of the practice of law.
27. After the execution of the search by the Search Team and, where necessary, the Filter Team, the Filter Team will review physical and electronic materials seized to identify and segregate documents or data containing potentially privileged information.
28. If the Filter Team determines the documents or data are not potentially privileged, they may be provided to the law enforcement personnel assigned to the investigation immediately. If at any point the law enforcement personnel assigned to the investigation subsequently identify any data or documents that they consider may be potentially privileged, they will cease the review of such identified data or documents and refer the materials to the Filter Team for further review by the Filter Team.
29. If the Filter Team determines that documents are potentially privileged or merit further consideration in that regard, a Filter Team attorney may do any of the following: (a) apply *ex parte* to the court for a determination whether or not the documents contain privileged material; (b) defer seeking court intervention and continue to keep the documents inaccessible to law enforcement personnel assigned to the investigation; or (c) disclose the documents to the potential privilege holder, request the privilege holder to state whether the potential privilege holder asserts privilege as to any documents, including requesting a particularized privilege log, and seek a ruling from the court regarding any privilege claims as to which the Privilege Review Team and the privilege-holder cannot reach agreement.